PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-078235
(43)Date of publication of application : 14.03.2000

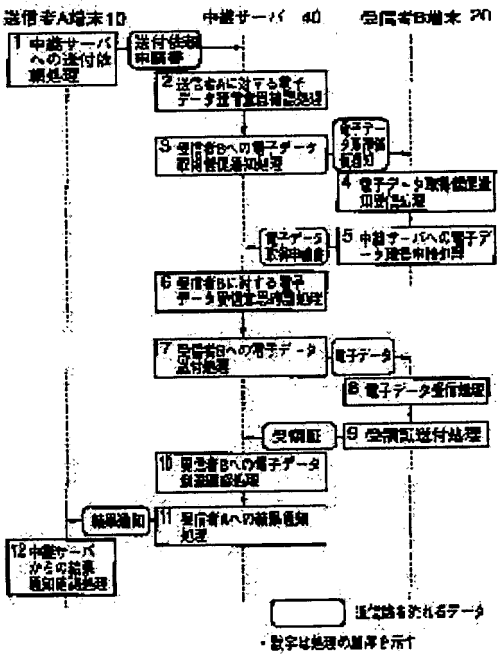
(51)Int.CI. H04L 29/08
G09C 1/00
H04L 12/66
H04L 12/54
H04L 12/58

(21)Application number : 10-241699
(22)Date of filing : 27.08.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HASHIMOTO SHOICHI

(54) ELECTRONIC DATA ARRIVAL WARRANTEE METHOD, ELECTRONIC DATA RELAY SYSTEM AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To certify the fact for a 3rd party that a sender A transmitted electronic data to a recipient B and that the latter had the intention of receiving the electronic data.
SOLUTION: A sender A transmits a transmission request, including electronic data and a name of a recipient B to a relay server 40, which stores the transmission request sheet and informs a recipient B of the storage of the electronic data addressed to the recipient B together with its identifier. The recipient B generates an acquisition application sheet and sends it to the server 40. The server 40 confirms that the acquisition application sheet is sent from the recipient B and a transmission destination of electronic data with the identifier matches the recipient B, stores the acquisition application sheet and transmits the electronic data designated by the identifier in the acquisition application sheet to the recipient B. The recipient B generates reception confirmation information, specifying the electronic data definitely and sends a receipt including the information and the identifier to the server 40, and the server 40 confirms that the reception confirmation information is identical to the electronic data designated by the identifier and stores the receipt.



LEGAL STATUS

[Date of request for examination] 20.10.2000
[Date of sending the examiner's decision of rejection] 21.05.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2002-11286
[Date of requesting appeal against examiner's decision of rejection] 20.06.2002
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－78235
（P2000－78235A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　29/08		Ｈ０４Ｌ　13/00	３０７Ａ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	
	６６０		６６０Ｇ	
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	
12/54			１０１Ｚ	

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平10－241699

(22)出願日　平成10年８月27日(1998.8.27)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　橋本　正一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

(54)【発明の名称】　電子データ到達保証方法、電子データ中継システム及びプログラム記録媒体

(57)【要約】
【課題】　送信者Ａが受信者Ｂへ電子データを送付した事実、Ｂが電子データを受理する意志があったことなどを第三者に対して証明可能とする。
【解決手段】　Ａは電子データとＢを含む送付依頼書を中継サーバ４０に送り、中継サーバは送付依頼書を保管し、Ｂ宛の電子データを保管していることをその識別子と共にＢへ通知する。Ｂは取得申請書を作り、サーバ４０へ送り、サーバ４０は取得申請書がＢから送られたもの、その識別子の電子データの送付先がＢと一致することを確認して、取得申請書を保管し、申請書の識別子で指定された電子データをＢへ送る。Ｂは電子データを一意に特定可能な受領確認情報を作り、これと識別子を含む受領書をサーバ４０へ送り、サーバ４０は受領確認情報が識別子の電子データと同一のものであることを確認して、受領証を保管する。

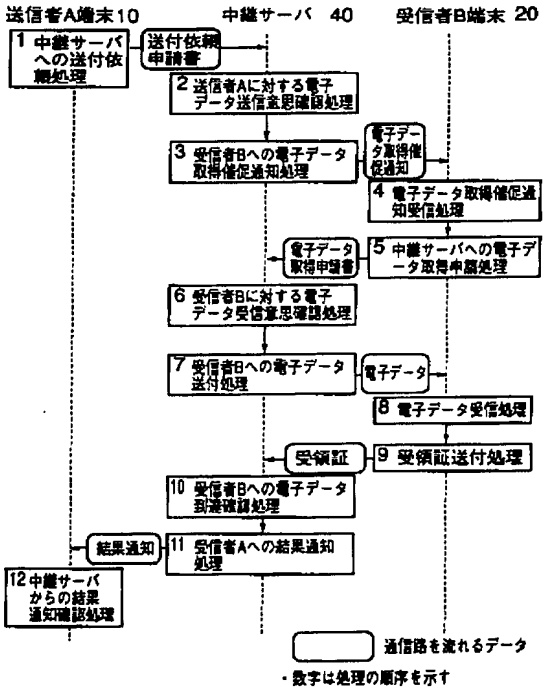


図　２　本発明における電子データ到達保証方法を実現するための処理の流れ

1

【特許請求の範囲】

【請求項１】　コンピュータネットワークを介して送信者Ａ端末が受信者Ｂ端末に電子データを送信する時、送信者Ａ端末と受信者Ｂ端末との間で電子データの送付を仲介し、その仲介事実を保証するための電子データ通信手段、公開鍵証明証取得手段、電子署名検証手段、電子データ保管手段及び受領確認情報確認手段を有する中継サーバと、

中継サーバに対して受信者Ｂ端末への送付を依頼するための電子データ編集手段、電子署名生成手段、電子データ通信手段と、中継サーバからの依頼に対する結果を確認するための電子データ表示手段とを有する送信者Ａ端末と、

中継サーバからの電子データの受理と引き換えに受理した証を中継サーバへ返すための電子データ編集手段、電子署名生成手段、電子データ通信手段及び、受領確認情報生成手段を有する受信者Ｂ端末と、

公開鍵証明証を配送する手段を有する認証システムとからなる電子データ中継システム。

【請求項２】　送信者端末において、電子データ編集手段を用いて送付対象電子データ及び送付先情報を含んだ送付依頼申請書を作成し、電子署名生成手段を用いて送付依頼申請書に対する送信者Ａの電子署名を生成し、電子データ通信手段を用いて電子署名が付与された送付依頼申請書を中継サーバへ送付し、

中継サーバにおいて、電子データ通信手段を用いて送信者端末が送付した送付依頼申請書を受理後、公開鍵証明証取得手段を用いて送信者Ａの公開鍵証明証を認証システムから取得し、電子署名検証手段を用いてこの公開鍵証明証内に含まれる公開鍵により送付依頼申請書に付与された電子署名を検証し、送付依頼申請書内に送付対象電子データ及び送付先情報が存在することを確認した後に、電子データ保管手段を用いて送付依頼申請書を保管することにより、送信者Ａが確かに送付依頼申請書に含まれる電子データを送付先情報として指定された受信者Ｂへ送付する意志があった事実を確認し、その証拠情報を保管することを特徴とする電子データ到達保証方法。

【請求項３】　中継サーバにおいて、電子データ通信手段を用いて中継サーバが受信者Ｂ宛の電子データを保管していること及びこれを取得するための識別子を受信者Ｂ端末に通知し、

受信者Ｂ端末において、電子データ通信手段を用いて中継サーバからのこの通知を受理した後、電子データ編集手段を用いて識別子に対応する電子データを取得するための電子データ取得申請書を作成し、電子署名生成手段を用いて電子データ取得申請書に対する受信者Ｂの電子署名を生成し、電子データ通信手段を用いて電子署名が付与された電子データ取得申請書を中継サーバへ送付し、

中継サーバにおいて、電子データ通信手段を用いて受信者Ｂ端末が送付した電子データ取得申請書を受理後、公開鍵証明証取得手段を用いて受信者Ｂの公開鍵証明証を認証システムから取得し、電子署名検証手段を用いてこの公開鍵証明証内に含まれる公開鍵により電子データ取得申請書に付与された電子署名を検証して、取得対象識別子に対応する電子データの送付先情報と電子データ取得申請書が一致していることを確認し、電子データ保管手段を用いて電子データ取得申請書を保管することにより、送信者Ａ端末が送付した電子データを受信者Ｂが受理する意志があった事実を確認し、その証拠情報を保管することを特徴とする電子データ到達保証方法。

2

【請求項４】　請求項３記載の方法において、

中継サーバにおいて、上記電子データ取得申請書を保管後に、電子データ通信手段を用いて送信者Ａ端末が送付を依頼した電子データを受信者Ｂ端末へ送付し、

受信者Ｂ端末において、電子データ通信手段を用いて中継サーバが送付した電子データを受信し、受領確認情報生成手段を用いて受理した電子データを一意に特定可能な受領確認情報を生成し、データ編集手段を用いて少なくとも受領確認情報と電子データ取得申請書で指定した識別子を含む受領証を生成し、電子署名生成手段を用いて受領証に対する受信者Ｂの電子署名を生成し、電子データ通信手段を用いて電子署名が付与された受領証を中継サーバへ送付し、

中継サーバにおいて、電子データ通信手段を用いて受信者Ｂ端末が送付した受領証を受理後、公開鍵証明証取得手段を用いて受信者Ｂの公開鍵証明証を認証システムから取得し、電子署名検証手段を用いてこの公開鍵証明証内に含まれる公開鍵により受領証に付与された電子署名を検証して、受領証内に示された識別子に対応する電子データの送付先情報と受領証の送付者が一致していることを確認し、受領確認情報確認手段を用いて受領証内に含まれる受領確認情報が識別子に対応する電子データと同一の電子データを指し示すことを確認し、電子データ保管手段を用いて受領証を保管することにより、送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理した事実を確認し、その証拠情報を保管することを特徴とする電子データ到達保証方法。

【請求項５】　請求項４記載の方法において、

中継サーバにおいて、上記受領証を保管後に、電子データ通信手段を用いて送付結果を送信者Ａ端末へ送付し、

送信者Ａ端末において、電子データ通信手段を用いて中継サーバから結果通知を受理し、電子データ表示手段を用いて受信者Ｂ端末へ電子データが到達したことを確認することにより、送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理した事実を、送信者Ａが確認することを特徴とする電子データ到達保証方法。

【請求項６】　送信者Ａ端末より受信した送付対象電子データ及び送付先情報を含む送付依頼申請書に対する電子署名をその送信者Ａの公開鍵により検証する処理と、

その検証に合格すると、上記送付依頼申請書を保管する処理と、
上記送付先情報である受信者Ｂ宛の電子データを保管していること及び、その電子データの識別子を受信者Ｂ端末へ送信する処理と、
を中継サーバのコンピュータに実行させるプログラムを記録した記録媒体。
【請求項７】　請求項６記載の記録媒体において、
受信者Ｂ端末より受信した電子データ取得申請書に対する電子署名を、受信者Ｂの公開鍵により検証する処理と、
その検証に合格すると、
上記電子データ取得申請書から取得した識別子と対応する電子データの送付先情報と、電子データ取得申請書の申請者が一致していることを確認する処理と、
その確認に合格すると、上記電子データ取得申請書を保管する処理と、
上記識別子と対応する上記保管した電子データを上記受信者Ｂ端末へ送信する処理と、
を上記コンピュータが実行するプログラムを上記プログラムが有することを特徴とする記録媒体。
【請求項８】　請求項７記載の記録媒体において、
受信者Ｂ端末より受信した受領証に対する電子署名を受信者Ｂの公開鍵により検証する処理と、
その検証に合格すると、受領証内に示された識別子に対応する電子データの送付先情報と、受領証の送付者が一致していることを確認する処理と、
受領証内に含まれる受領確認情報が、識別子に対応する保管中の電子データと同一の電子データを指し示すことを確認する処理と、
これらの確認に合格すると、受領証を保管する処理と、
を上記コンピュータが実行するプログラムを上記プログラムが有することを特徴とする記録媒体。
【請求項９】　請求項８記載の記録媒体において、
上記受領証を保管後に、送付結果を送信者Ａ端末へ送付する処理を上記コンピュータが実行するプログラムを上記プログラムが有することを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コンピュータネットワーク上でＥＤＩ（電子データ交換）やＥＣ（電子商取引）を実現するために必要となる電子データの送受信方式において、送付した電子データを確かに通信相手が受理したことを確認する方法及び、データの中継システム及びプログラム記録媒体に関するものである。
【０００２】
【従来の技術】コンピュータネットワークを介して電子データを送受信する場合に、なりすましや改竄（かいざん）などの脅威を防御し、受信者が電子データの送信元の本人性を確認する方式として、電子署名通信が一般に

用いられている。この電子署名通信を実現する暗号技術としては、公開鍵暗号方式であるＲＳＡやＥＳＩＧＮなどが広く知られているところとなっており、送信者側における電子署名生成手段と、受信者側における電子署名検証手段を対で利用することにより電子署名通信が実現される。また公開鍵暗号方式を用いた電子署名通信において、署名付与者の本人性を確実に確認するための方法としては、認証システムと呼ばれる大三者機関が発行する公開鍵証明証により、その所有者が保証された公開鍵を用いて署名検証を行う方法が世の中で広く知られるところとなっている。
【０００３】さて、この電子署名通信が利用可能な状況において、送信者Ａと受信者Ｂがコンピュータネットワークを介して電子データを送受信する場合に、送付した電子データが確かに受信者Ｂに受理されたことを送信者Ａが確認可能となる一般的な方法としては、次の手法が考えられる。即ち図４に示すように、送信者Ａ端末１０における電子データ送付処理において、電子データ編集手段１１１で送信すべき電子データを編集し、この電子データに対し、電子署名生成手段１１２で電子署名を作成し、この署名を電子データに付け電子データ通信手段１１３により、受信者Ｂ端末２０へ送信する。
【０００４】受信者Ｂ端末２０における電子データ受信処理において、電子データ通信手段２１３により電子データを受信し、公開鍵証明証取得手段２１４により認証システム３０から送信者Ａの公開鍵証明証を受領し、その公開鍵により、電子データ署名検証手段２１５で、受信電子データの署名を検証し、その検証に合格すると、受信電子データを電子データ保管手段２１６に保管する。
【０００５】その後、受信者Ｂ端末２０は受領証作成処理において、電子データ編集手段２１１により、電子データを受理したことを通知する受領証を作成し、その受領証に対する受信者Ｂの電子署名を電子署名生成手段２１２で生成し、その署名を受領証に付けて電子データ通信手段２１３により送信者Ａ端末１０へ送信する。最後に送信者Ａ端末１０における受領証確認処理において、電子データ通信手段１１３で受領証を受信し、公開鍵証明証取得手段１１４で認証システム３０から受信者Ｂの公開鍵証明証を取得し、その公開鍵を用いて電子データ署名検証手段１１５で受領証に対する署名を検証し、その検証に合格すると、受信した受領証を電子データ保管手段１１６に保管する。
【０００６】ここで、送受信される電子データや受領証に対しては、データを送付する側で電子署名の付与を、受信する側で電子署名の検証を行い、改竄やなりすましがないことを受信側において確認する。また受領証の構成内容は、送信者Ａと受信者Ｂとの間であらかじめ任意に規定されたものが使用されている。
【０００７】

【発明が解決しようとする課題】送信者Ａ端末１０が送付した電子データを確かに受信者Ｂ端末２０が受理したことを、受信者Ｂ端末２０が送付する受領証を用いて送信者Ａ端末１０が確認する場合、従来方法においては、送信者Ａ端末１０が送付した電子データと受信者Ｂ端末２０が作成する受領証とが関連付けられていないため、当事者以外の第三者が、この受領証によって受信者Ｂ端末２０による対象電子データの受理の事実を確認することができない。したがって、後日、受信者Ｂが悪意を持って故意に送信者Ａ端末１０から送付された電子データの受信事実を否認するなどの当事者間における紛争が生じた場合、紛争を解決するために第三者に対して提示可能な証拠情報がなく、電子データが受信者Ｂ端末２０へ送付された事実を第三者に対して証明する手段がない。

【０００８】また従来技術において受領証が送信者Ａ端末１０に送付されてこない場合には、送信者Ａ端末１０が送付した電子データを受信者Ｂ端末２０が受理した事実はもちろん、送信者Ａ端末１０が受信者Ｂ端末２０に対して電子データを送付した事実や、受信者Ｂ端末２０が電子データを受理する意志があった事実を確認してこれを証明することができないという問題があった。

【０００９】そこでこの発明では、送信者Ａ端末が受信者Ｂ端末へ電子データを送付する過程において、送信者Ａ端末が受信者Ｂ端末に対して電子データを送付した事実及び、受信者Ｂ端末が電子データを受理する意志があった事実及び、送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理した事実を確認し、これらの事実を当事者以外の第三者に対して証明可能となる電子データ到達保証方法を提供し、またこの方法を実現する電子データ中継システムを構築すること、更にそのために各部で用いるプログラム記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】コンピュータネットワークを介して送信者Ａ端末が受信者Ｂ端末に電子データを送付する時、送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理したことを確認し、この事実を当事者以外の第三者に対して証明可能とするために、この発明では、図１に示す装置構成に示すように電子データの送受信に中継サーバ４０を介在させ、この中継サーバ４０が送信者Ａ端末１０から受信者Ｂ端末２０へ電子データを中継する過程において、（Ａ）送信者Ａが確かに電子データを受信者Ｂ端末２０へ送付する意志があった事実及び、（Ｂ）送信者Ａ端末が送付した電子データを受信者Ｂが受理する意志があった事実及び、（Ｃ）送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理した事実を確認し、それぞれ確認に用いた電子情報を証拠情報として保管するところに特徴がある。以下では、送信者Ａ端末１０と受信者Ｂ端末２０の間に介在した中継サーバ４０において、（Ａ）～（Ｃ）の事実を確認しその証拠情報を保管する手段について、図２を用いて説明する。

【００１１】（Ａ）送信者Ａが確かに電子データを受信者Ｂ端末へ送付する意志があった事実の確認及びその証拠情報の保管手段

１：中継サーバへの送付依頼処理

送信者Ａ端末１０は、送付対象である電子データと、その送付先情報とを最低限含んだ送付依頼申請書を作成し、これに自端末（送信者Ａ端末）１０が作成したことの証を含めて中継サーバ４０へ送付する。

２：送信者Ａに対する電子データ送信意志確認処理

中継サーバ４０は、１の送付依頼申請書を受理し、これが確かに送信者Ａ端末１０から送付されてきたこと及び、送付対象電子データ及び送付先情報の存在を確認し、この送付依頼申請書を保管する。

【００１２】以上により、中継サーバ４０において、送信者Ａが確かに送付依頼申請書に含まれる電子データを、送付先情報で示された受信者Ｂ端末へ送付する意志があった事実を確認し、その証拠情報の保管を実現する。

（Ｂ）送信者Ａ端末が送付した電子データを受信者Ｂが受理する意志があった事実の確認及びその証拠情報の保管手段

３：受信者Ｂ端末への電子データ取得催促通知処理

中継サーバ４０は、送信者Ａ端末から受理した受信者Ｂ端末宛の電子データを保管していること及びこれを取得するための識別子を受信者Ｂ端末に対して通知し、これを取得することを促す。

４：電子データ取得催促通知受信処理

受信者Ｂ端末は、中継サーバ４０からの３の通知を受理する。

５：中継サーバへの電子データ取得申請処理

受信者Ｂ端末２０は、識別子に対応する電子データを取得するための電子データ取得申請書を作成し、これに自端末（受信者Ｂ端末）２０が作成したことの証を含めて中継サーバ４０へ送付する。

６：受信者Ｂに対する電子データ受信意志確認処理

中継サーバ４０は、５の取得申請書を受理し、これが確かに受信者Ｂ端末２０から送付されてきたこと及び、この取得申請書に示された識別子に対応する電子データの送付先情報が、取得申請書の送付者である受信者Ｂ端末と一致していることを確認し、この取得申請書を保管する。

【００１３】以上により、中継サーバ４０において、送信者Ａ端末１０が送付した電子データを受信者Ｂが受理する意志があった事実を確認し、その証拠情報の保管を実現する。

（Ｃ）送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理した事実の確認及びその証拠情報の保管手段

７：受信者Ｂ端末への電子データ送付処理
中継サーバ４０は、受信者Ｂ端末２０に対して電子データ取得申請書で指定された識別子に対応する電子データを送付する。
８：電子データ受信処理
受信者Ｂ装置２０は、７で送付された電子データを受理する。
９：受領証送付処理
受信者Ｂ端末は、８で受理した電子データを一意に特定可能となる受領確認情報を生成し、少なくとも受領確認情報と取得申請書で指定した識別子を含む受領証を作成後、これに自端末（受信者Ｂ端末）２０が作成したことの証を含めて中継サーバ４０へ送付する。
１０：受信者Ｂ端末への電子データ到達確認処理
中継サーバ４０は９で送付された受領証を受理し、これが確かに受信者Ｂ端末から送付されてきたこと及び、この受領証に含まれる識別子に対応する電子データの送付先情報が、受領証の送付者である受信者Ｂ端末２０と一致していることを確認するとともに、受領証内に含まれる受領確認情報が、識別子に対応する電子データと同一の電子データを指し示すことを確認し、この受領証を保管する。
【００１４】以上により、中継サーバ４０において、送信者Ａ端末１０が送付した電子データを受信者Ｂ端末２０が確かに受理した事実を確認し、その証拠情報の保管を実現する。そして、１～１０の処理の後に、中継サーバ４０における１１送信者Ａ端末１０への結果通知処理において、中継サーバ４０から受信者Ｂ端末２０への電子データの送付結果を通知し、送信者Ａ端末１０における１２中継サーバ４０からの結果通知確認処理において、１１で送付された結果通知を受理し、受信者Ｂ端末２０への電子データの到達を確認することにより、送信者Ａ端末１０が送付した電子データを受信者Ｂ端末２０が確かに受理した事実を、送信者Ａ端末１０が確認することが可能となる。
【００１５】
【発明の実施の形態】この発明を実現するための具体的な実施例を図１、図３に示す。
１：中継サーバへの送付依頼処理
送信者Ａ端末１０は、受信者Ｂ端末２０への電子データの送付を中継サーバ４０に依頼するため、電子データ編集手段１１１を用いて送付対象である電子データ及び送付先情報を最低限含んだ送付依頼申請書を作成し、電子署名生成手段１１２を用いてこの申請書に対する送信者Ａの電子署名を生成し、電子データ通信手段１１３を用いて電子署名が付与された送付依頼申請書５１を中継サーバ４０へ送付する。
【００１６】電子データ編集手段１１１は、コンピュータシステムが一般的に提供するエディタ機能やファイル読み込み機能を利用することにより、送付対象である電子データ及び送付先情報を最低限含んだ送付依頼申請書を作成することが可能である。また、電子署名生成手段１１２は、既存のＲＳＡやＥＳＩＧＮなどの公開鍵暗号技術を用いて実現可能であり、公開鍵暗号技術で必要となる秘密鍵と公開鍵のうち、電子署名生成者のみが知りうる秘密鍵を用いて署名対象である電子データを暗号化することにより、電子データに対する電子署名を生成することが可能となる。さらに、電子データ通信手段１１３は、コンピュータシステムが一般的に提供するファイル転送機能やファイル受信機能などを利用することにより容易に実現可能である。
２：送信者Ａに対する電子データ送信意志確認処理
中継サーバ４０は、送信者Ａが確かに電子データを受信者Ｂ端末２０へ送付する意志があった事実を確認するため、電子データ通信手段４１１を用いて送信者Ａ端末１０から送付依頼申請書５１を受理後、公開鍵証明証取得手段４１２を用いて送信者Ａの公開鍵証明証を認証システム３０から取得し、電子署名検証手段４１３を用いてこの公開鍵証明証内に含まれる公開鍵により送付依頼申請書５１に付与された電子署名を検証して、送付依頼申請書５１の送付者が確かに送信者Ａであることを確認する。そして申請書５１内に送付対象電子データとその送付先情報が含まれていることを確認した後、ここで確認した事実の証拠情報を保管するため、電子データ保管手段４１４を用いて送付依頼申請書５１を２次記憶媒体へ保管する。
【００１７】ここで、公開鍵証明証取得手段４１２は、公開鍵暗号技術で必要となる秘密鍵と公開鍵のうち、一般利用者に公開するための公開鍵を第三者機関である認証システム３０へあらかじめ登録しておき、署名検証において署名検証対象者の公開鍵を必要とする場合に、認証システム３０に対して利用者名等を検索キーとして公開鍵証明証の検索を依頼することにより、必要な公開鍵証明証の取得が実現可能であり、これらの処理は、認証システム３０が一般に保持する公開鍵証明証配送機能や既存のディレクトリ参照技術などを用いて実現可能である。また、電子署名検証手段４１３は、電子署名生成手段１１２と対で利用される手段であり、既存の暗号技術を用いて実現可能である。この手段は、公開鍵証明証取得手段４１２を利用して取得した公開鍵証明証内に含まれる公開鍵と、検証対象である電子署名及び署名の生成対象である電子データを入力として、対象電子データに付与された電子署名が、確かに公開鍵証明証内に示された公開鍵の所有者により生成されたものであることの検証を可能とする。さらに、電子データ保管手段４１４は、コンピュータシステムが一般的に提供するファイル入出力機能などを利用することにより容易に実現可能である。
【００１８】以上の処理と手段により、中継サーバ４０において、送信者Ａが確かに対象電子データを受信者Ｂ

端末２０へ送付する意志があった事実を確認し、その証拠情報の保管が実現可能となる。

３：受信者Ｂ端末への電子データ取得催促通知処理

中継サーバ４０は、送信者Ａ端末１０が指定した送付先の受信者Ｂ端末２０に対して、中継サーバ４０が受信者Ｂ端末２０宛の電子データを保管していること及びこれを取得するための識別子よりなる電子データ取得催促通知５２を、電子データ通信手段４１１を用いて通知する。

４：電子データ取得催促通知受信処理

受信者Ｂ端末２０は、電子データ通信手段２１３を用いて３で送付された通知５２を受理する。

５：中継サーバへの電子データ取得申請処理

受信者Ｂ端末２０は、中継サーバ４０に保管されている受信者Ｂ端末２０宛の電子データを取得するため、電子データ編集手段２１１を用いて識別子に対応する電子データを取得するための電子データ取得申請書を作成し、電子署名生成手段２１２を用いて電子データ取得申請書に対する受信者Ｂの電子署名を生成し、電子データ通信手段２１３を用いて電子署名が付与された電子データ取得申請書５３を中継サーバ４０へ送付する。

６：受信者Ｂに対する電子データ受信意志確認処理

中継サーバ４０は、受信者Ｂが確かに送信者Ａ端末１０から送付された電子データを受信する意志があった事実を確認するため、電子データ通信手段４１１を用いて受信者Ｂ端末２０から電子データ取得申請書５３を受理後、公開鍵証明証取得手段４１２を用いて受信者Ｂの公開鍵証明証を認証システム３０から取得し、電子署名検証手段４１３を用いてこの公開鍵証明証内に含まれる公開鍵により電子データ取得申請書５３に付与された電子署名を検証して、電子データ取得申請書５３で指定された識別子に対応する電子データの送付先情報が、電子データ取得申請書５３の送付者である受信者Ｂと一致していることを確認する。その後、ここで確認した事実の証拠情報を保管するため、電子データ保管手段４１４を用いて電子データ取得申請書５３を２次記憶媒体へ保管する。

【００１９】以上の処理と手段により、中継サーバ４０において、送信者Ａが送付した電子データを受信者Ｂが受理する意志があった事実を確認し、その証拠情報の保管が実現可能となる。

７：受信者Ｂ端末への電子データ送付処理

中継サーバ４０は、電子データ通信手段４１１を用いて電子データ取得申請書５３で指定された識別子に対応する電子データ５４を受信者Ｂ端末２０へ送付する。

８：電子データ受信処理

受信者Ｂ端末２０は、電子データ通信手段２１３を用いて中継サーバ４０が送付した電子データを受信する。

９：受領証送付処理

受信者Ｂ端末２０は、電子データを受理したことを中継サーバ４０に対して通知するための受領証を送付するため、受領確認情報生成手段２１７を用いて受理した電子データを一意に特定可能な受領確認情報を生成し、データ編集手段２１１を用いて少なくとも受領確認情報と取得申請書で指定した識別子を含む受領証を生成する。そして、電子署名生成手段２１２を用いてこの受領証に対する受信者Ｂの電子署名を生成し、電子データ通信手段２１３を用いて電子署名が付与された受領証５５を中継サーバ４０へ送付する。

【００２０】ここで受領確認情報生成手段２１７は、どの電子データを受理したのかを一意に特定する情報を生成するための手段であり、この手段は、例えばハッシュ化技術を用いて、受理した電子データに対するハッシュ値を生成し、これを受領確認情報とすることにより実現可能である。このことは、受理した電子データと、これを元に算出したハッシュ値が、確率統計上極めて１対１の関係を保持することが可能となるためである。またこのハッシュ化技術は、既存のＭＤ５やＳＨＡ－１などが世の中で広く知られるところとなっている。

１０：受信者Ｂ端末への電子データ到達確認処理

中継サーバ４０において、受信者Ｂ端末２０が確かに送信者Ａ端末１０が送付した電子データを受理した事実を確認するため、電子データ通信手段４１１を用いて受信者Ｂ端末２０から受領証５５を受理後、公開鍵証明証取得手段４１２を用いて受信者Ｂの公開鍵証明証を認証システムから取得し、電子署名検証手段４１３を用いてこの公開鍵証明証内に含まれる公開鍵により受領証５５に付与された電子署名を検証して、受領証５５の送付者が受信者Ｂ端末２０であることを確認し、さらにこの受信者Ｂ端末２０が、受領証５５内に含まれる識別子に対応する電子データの送付先情報と一致していることを確認する。続いて、受信者Ｂ端末２０が受理した電子データ５４が、確かに送信者Ａ端末１０が送付依頼した電子データであることを確認するため、受領確認情報確認手段４１５を用いて受領証５５内に含まれる受領確認情報が識別子に対応する電子データと同一の電子データを指し示すことを確認する。その後、ここで確認した事実の証拠情報を保管するため、電子データ保管手段４１４を用いて受領証５５を２次記憶媒体へ保管する。

【００２１】ここで、受領確認情報確認手段４１５は、受信者Ｂ端末２０が受理した電子データが、送付した電子データと同一であることを確認するための手段であり、受領確認情報生成手段２１７で示したハッシュ化技術を用いて、電子データの送信者である中継サーバ４０において、受信者Ｂ端末２０へ送付した電子データに対するハッシュ値を生成し、これと受信者Ｂ端末２０から受理した受領確認情報とを比較し、これらが一致することを確認することにより実現する。

【００２２】以上の処理と手段により、中継サーバ４０において、送信者Ａ端末１０が送付した電子データを受

11

信者Ｂ端末２０が確かに受理した事実を確認し、その証拠情報の保管が実現可能となる。

１１：受信者Ａ端末への結果通知処理

中継サーバ４０は、送信者Ａ端末１０に対して受信者Ｂ端末２０への電子データ送付の結果を通知するため、電子データ通信手段４１１を用いて送付結果通知５６を送信者Ａ端末１０へ送付する。

１２：中継サーバからの結果通知確認処理

送信者Ａ端末１０は、電子データ通信手段１１３を用いて１１で送付された結果通知５６を受理し、電子データ表示手段１１７を用いて受信者Ｂ端末２０へ電子データが到達したことを確認する。

【００２３】ここで電子データ表示手段１１７は、コンピュータシステムが一般的に提供するエディタ機能などを利用することにより容易に実現可能である。以上の処理と手段により、送信者Ａ端末１０が送付した電子データを受信者Ｂ端末２０が確かに受理した事実を、送信者Ａが確認することが可能となる。

【００２４】

【発明の効果】以上の説明から明らかであるように、この発明の方法とそれを実現する手段によって、送信者Ａ

12

端末と受信者Ｂ端末の間で送受信された電子データに対して、送信者Ａが電子データを受信者Ｂ端末に対して送付する意志があった事実及び、送信者Ａ端末が送付した電子データを受信者Ｂが受理する意志があった事実及び、送信者Ａ端末が送付した電子データを受信者Ｂ端末が確かに受理した事実を、後日、中継サーバが内部に保管している情報を提示することにより、外部の第三者に対して証明することが可能となる。また、中継サーバが送信者端末と受信者端末の間に介在して電子データの送受信の確認及び制御を行っているため、電子データの送受信を行う当事者の意志によらない確実な電子データの送達が可能となる。

【図面の簡単な説明】

【図１】この発明の装置構成を示すブロック図。

【図２】この発明における中継サーバを介した電子データ到達保証方法を実現するための処理の流れを示す図。

【図３】この発明を実現するための具体的実施例の処理の流れを、必要な手段とともに示す図。

【図４】Ａは従来技術による電子データの到達確認方法のシステム構成を示す図、Ｂはその処理手順を示す図である。

【図１】

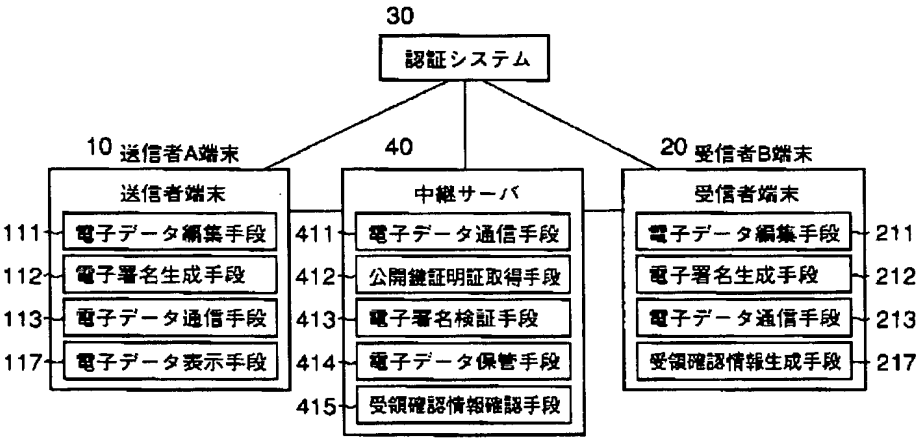


図　１　本発明における装置構成

【図２】

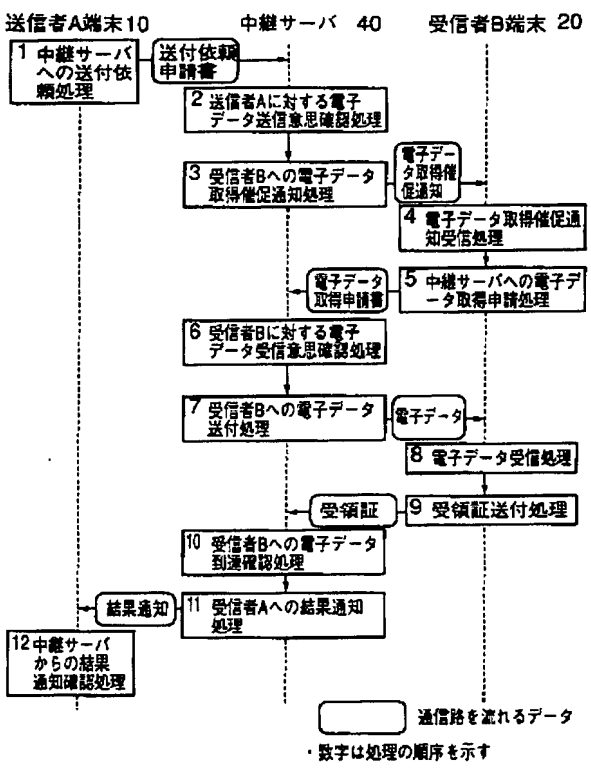


図　2　本発明における電子データ到達保証方法を実現するための処理の流れ

【図３】

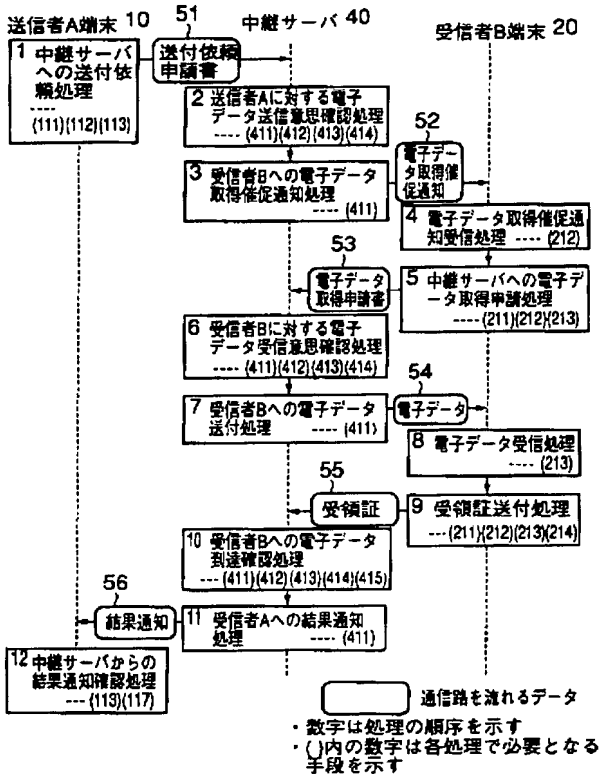


図　3　本発明を実現する具体的な実施例

【図４】

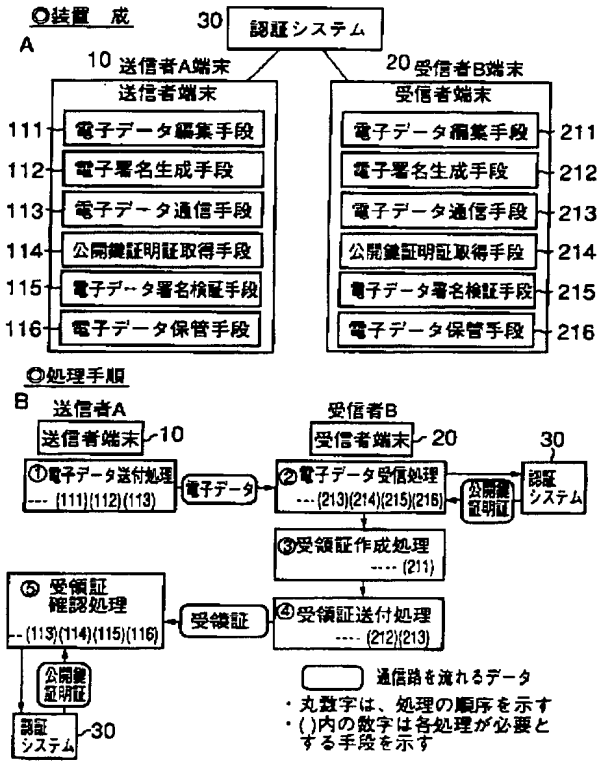


図　4　従来技術における電子データ到達確認方法

フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/58			